Weekly Report

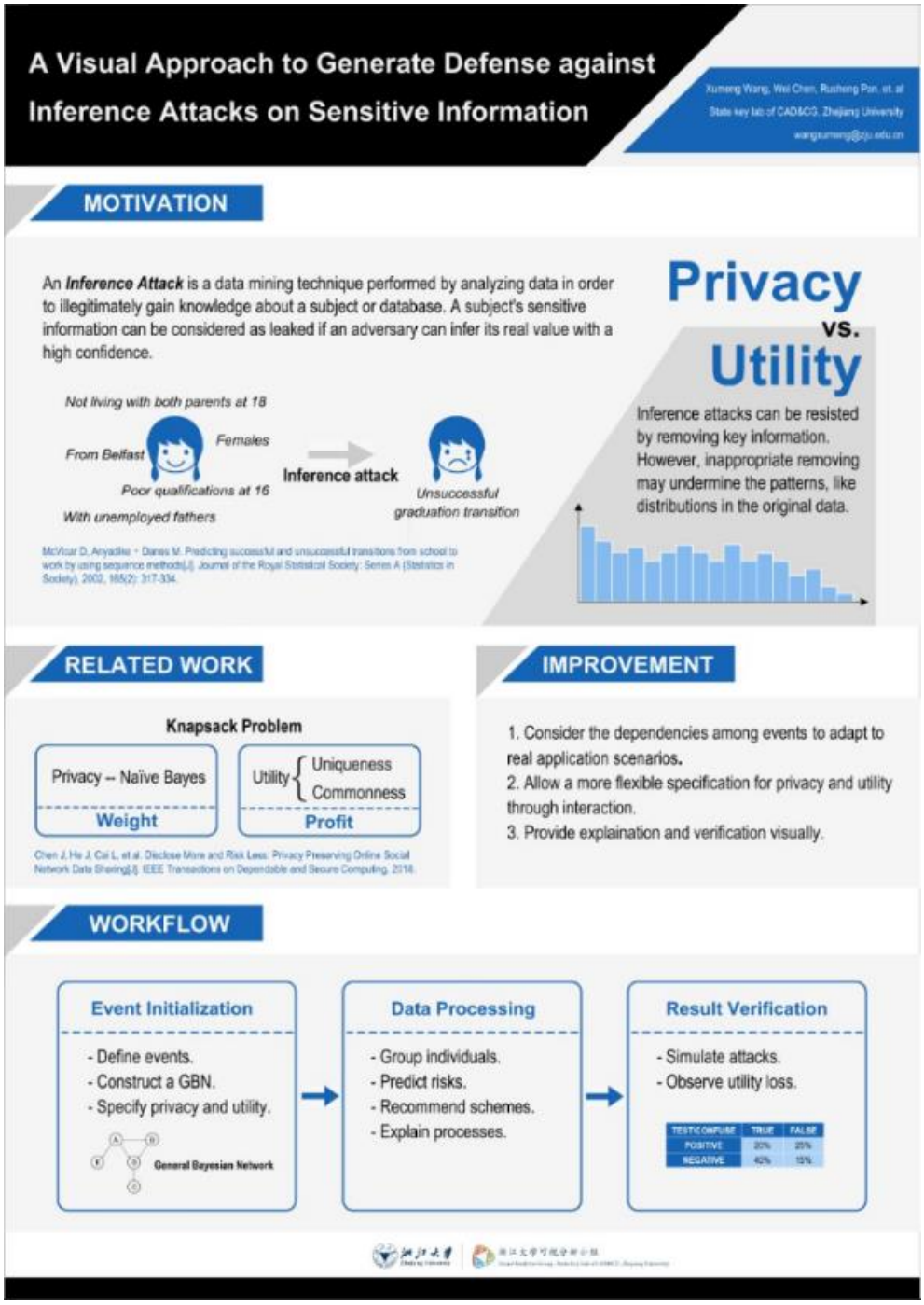
1 Done

1.1 Article

- Translate the text in the figures into Chinese.
- Ask Donming to proofread and improve words.

1.2 Poster

I designed the poster for the Exchange Forum.



1.3 Presentation

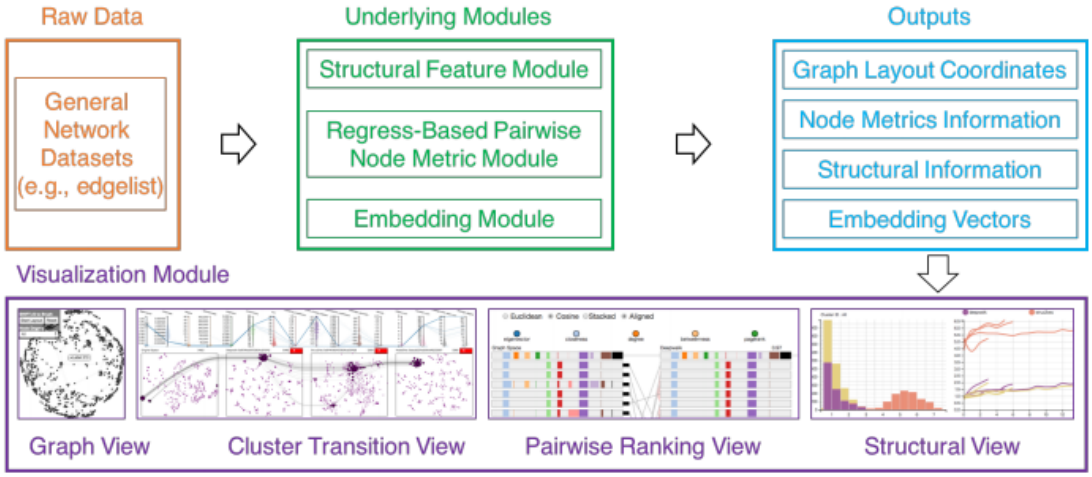
Yiran presented our vast paper to Bosch. Based on her feedback, I improved the slides.

1.4 Project

We defined the data exchange interfaces between front end and back end.

1.5 Paper Reading

EmbeddingVis: A Visual Analytics Approach to Comparative Network Embedding Inspection



In this system, users can compare three modules:
- The embedding module applies the network embedding models to the dataset.
- The regression-based pairwise node metric module extracts the node metrics from the data and generates the feature importance for each metric.
- The structural feature module extracts the ‘focal node’-‘neighborhood’ information of the network.

The outputs of these modules are fed into the visualization module, which provides three levels of analysis, namely, the cluster level as the cluster transition view, the instance level as the pairwise ranking view, and the structural level as the structural view. This module also provides rich real-time interactions that enable the experts to effectively inspect the embedding results in a fine-grained comparative manner.

Visualizing Dataflow Graphs of Deep Learning Models in TensorFlow

This is a design study of the TensorFlow machine intelligence platform.

Identifying inference attacks against healthcare data repositories

This work identifies a dangerous inference attack against naive suppression based approaches that are used to protect sensitive information.

One potential solution is through query auditing. Query auditing keeps track of the information revealed through queries. When done in an online fashion, submitted queries are checked in a continuous manner, to prevent inference disclosure. This is accomplished by combining responses to past queries with the response to the current query to determine if a breach occurs by responding to the new query. Another potential solution is through the use of more formal privacy protection models.

1.6 Searching for the Report Given by Prof. Yang Qiang

https://zhuanlan.zhihu.com/p/42646278

- Differential privacy does not have enough capacity to provide privacy protection that meets the requirements of the GDPR.
- Only interpretable automatic models can be used for decision making. I think this opinion proves the need for visualization, especially the part for explanation.
-"Federal Learning" means a network in which both sides A and B can participate in federal learning without specifically exchanging the original data and without revealing the difference in the user ID. In this network, a common model can be established, and the parameters of this model can be held independently. In other words, both models can grow, but they don't communicate directly with each other. In this way, the user's sample and user characteristics are not leaked, and most of the requirements of the GDPR have been met.

1.7 Mid-term Answering

Got ready for mid-term answering.

2 Work Hours

Monday	9:00-11:30	12:30-17:30	-
Tuesday	9:00-11:00	12:00-17:20	19:00-20:30
Wednesday	9:00-11:10	12:30-17:00	-
Thursday	9:00-11:00	12:30-17:20	19:00-20:30
Friday	9:00-11:10	12:30-17:00	19:00-20:30
Saturday	10:00-11:30	14:00-17:00	-
Sunday	-	15:00-17:00	19:00-20:30

3 Progress

Item	Deadline	Current progress	Remark
Vis presentation	10.24	Nearly done.	
Go abroad	11.10	Bought the ticket.	
Privacy program	-	Define interfaces for data exchange.	
Article	10.30	Nearly done.	